

## **Tab B Return on Investment Program Funding Application for FY 2013**

### **Contact Information:**

#### **Funding to be requested (select only one):**

☒ **IT Enterprise Solution project**

☐ **Agency Specific IT project**

Date: 8/31/2011

Agency Name: DAS on behalf of CIO  
Security Subcommittee

Project Name: Endpoint Protection

Agency Manager: Jeff Franklin

Agency Manager Phone Number / E-Mail: 281-4820, jeff.franklin@iowa.gov

Executive Sponsor (Agency Director or  
Designee): Lorrie Tritch

**Amount of Funding Requested:** \_\$450,000\_\_\_\_\_

### **Section I: Project Description:**

Project: Enterprise Endpoint Protection

Endpoint Definition: Endpoints on a network include PC's, laptops, tablets and other devices where users connect to the government network.

Appropriate endpoint security measures are one of the critical elements in protecting an IT environment. Traditionally, antivirus was sufficient to protect endpoints on the network. However, in the past few years, cyber attacks have become much more sophisticated and now require greater protection measures. Some additional security measures include encryption, anti-malware, anti-phishing, spyware protection, desktop firewalls, USB Control, host-based intrusion prevention and detection and data leakage protection. Many of these security products can be procured in a suite; however, some are separate software procurements. The goal of the project is to identify and implement the necessary controls to secure endpoints in a consistent manner.

State of Iowa agencies maintain a variety of different endpoint protections products. Some of which are very comprehensive and some of which are inadequate. The current model is the most expensive to maintain and the most difficult to secure. In today's model we need to maintain expertise in multiple products; we achieve no economies of scale for volume purchasing and have no consistent way to deploy, manage or secure endpoints solutions. This project is designed to standardize the security protections on all endpoints.

The CIO Security Subcommittee has formed an endpoint protection cross-agency working group to research and identify the most appropriate solution(s) for the State of Iowa agencies. Once an enterprise solution(s) has been identified, the

working group will recommend an implementation plan. Procurement will be accomplished through existing contracts or with the RFP process.

This initiative supports multiple requirements within the State of Iowa Enterprise Security Standards. These are located at:

<http://secureonline.iowa.gov/links/index.html>

Reducing the number of endpoint solutions and centrally managing the solution for all agencies within state government is the most cost effective approach. In addition, centralizing management of endpoint security will improve the integration of security efforts and communication, increase the effectiveness of policy enforcement and reduce the risk of agencies implementing non-compliant endpoints on the State's network.

These efforts are supported in SF2088, EO20 and EO26 and will support the Governor's Leadership Agenda to decrease cost in State government by at least 15%. This strategic initiative is also supported in the DAS Strategic Plan to consolidate state services. New York recently consolidated its' endpoint solutions and estimates spending on endpoint protection security products will drop 75 percent over the next three years.

## **Section II: Expected Results**

The key benefit to the State of Iowa is the improved protection of citizen data. This data is accessed through endpoints on agency networks. A primary attack vector for networks is through the compromise of endpoints. This can occur when a user clicks on a malicious link, responds to a phishing e-mail or visits an infected website. Once a user's credentials and endpoint computer are compromised, the attacker can establish a presence in the network and conduct more sophisticated covert attacks, retrieve confidential data and disrupt operations. This is an enterprise project and the solution(s) will benefit all agencies and users.

All State agencies handle confidential data in one form or another. It may be Social Security numbers, financial data, attorney opinions or medical information. State and Federal laws require the proper handling and protection of this data. This project supports these requirements.

New processes and possibly a new organizational support structure will be necessary in order to provide endpoint security on a centrally managed basis. This model has been proven to work in other states and expertise exists within the State of Iowa agencies to accomplish this. Initiatives are already underway which will centralize IT resources within the State. This project supports that initiative.

In addition, procuring an enterprise endpoint protection product, the State of Iowa will achieve savings by purchasing in volume and centralizing management.

## **Section III: Financial Analysis**

Agency funding already exist for the procurement of endpoint protection. This funding will be used to manage the project, procure new software and/or augment

existing endpoint protection software. Approximately \$150,000 will be used for contracted resources to oversee and manage the project and \$300,000 will be used towards the purchase of endpoint security products.

Large reductions in operating costs will be achieved during centralization and consolidation of endpoint protection among the state agencies. Symantec and McAfee both have worked with other states and have reported savings as high as 75 percent per endpoint. Symantec just completed a case study of a state similar in size to Iowa and reported a savings of \$133.33 per endpoint on 30,000 endpoints. McAfee reported in a case study of New York, savings of \$ 26.80 per endpoint a year on 250,000 endpoints over the next three years. This represents a total savings for New York of almost 20 million dollars over the next three years.

ROI examples:

PC Support:

10% of 20,000 of users have an infected PC per year = 2000  
8 hours of support per infected PC  
\$40.00 per hour spent on support  
Annual cost = \$640,000

Breach:

One user's PC with access to a database is infected  
Resulting is a breach of 100,000 records  
Conservative estimate of cost per record breached = \$20  
Cost to the State = \$2,000,000

Reduction in Endpoint Security Spending: (used in financial ROI Enclosure)

Estimated Current Cost = \$125 per device  
New cost due to standardization, central management and volume purchasing = \$100  
20,000 PC's x \$25 = \$500,000 annually

Reoccurring costs estimated at 5 percent of \$300,000 = \$15,000

Without a centralized solution, there is no way to guarantee all endpoints are protected at all agencies. The cost of a security breach can easily reach into the millions of dollars. In addition, without centralization the State continues to pass on possible significant cost saving measures. Further, as mobile technology advances the need for new endpoint solutions will follow. Without an enterprise-wide solution the possibility of even more products and expenses within the state could escalate as agencies diversify on future endpoint products.

## **Section IV: Auditable Outcome Measures**

**(Note that Section IV is not used in the scoring of the project)**

1. Improved customer service
  - Policy enforcement (measured by annual assessment)
  - Reduction in number of incidents (month to month, year to year comparison)
2. Citizen impact
  - Economies of scale with volume purchasing (saving tax dollars)

- Reduction in number of incidents results in improvements toward protecting citizen's data.
- 3. Cost Savings
  - Amount saved per endpoint based on actual protection needed
- 4. Project reengineering - unknown
- 5. Source of funds (Budget %) - unknown
- 6. Tangible/Intangible benefits
  - Reduction in support calls associated with intrusions
  - Reduction in endpoint intrusions

## Enclosure One – Financial Analysis

**Enclosure One, Financial Analysis Spreadsheet to Return on Investment (ROI) Program  
Funding Application**

Agency Name:	DAS / CIO Security Subcommittee
Application Name:	Enterprise Endpoint Protection

**Table One: Estimated Project Cost**

	FY13	FY14	FY15	FY16	FY17
Development and Implementation Costs	\$450,000	\$0	\$0	\$0	\$0
Recurring Costs	\$0	\$15,000	\$15,000	\$15,000	\$15,000
Total Costs	\$0	\$15,000	\$15,000	\$15,000	\$15,000

**Table Two: Percentage of Costs From**

General Fund					
Federal or other funding		\$15,000	\$15,000	\$15,000	\$15,000
Pooled Technology Fund	\$450,000				

**Table Three: Projected Reduction in Expense**

For Requesting Agency	\$500,000	\$500,000	\$500,000	\$500,000	\$500,000
For Other State Agencies	\$0	\$0	\$0	\$0	\$0
TOTAL Cost Reductions	\$500,000	\$500,000	\$500,000	\$500,000	\$500,000

**Table Four: Calculated Estimated Return on Investment**

Total projected cost from table one	\$450,000	\$15,000	\$15,000	\$15,000	\$15,000
Total projected cost reductions from table three	\$500,000	\$500,000	\$500,000	\$500,000	\$500,000
Projected Net Benefit to the State of Iowa	\$50,000	\$485,000	\$485,000	\$485,000	\$485,000